WebCrawler®

Web Search Yellow Pages White Pages

Web Pages Photos News

RSA "chinese remainder" public private Search

Exact Phrase

Advanced Search
Preferences
Tools & Tips

Now Searching: Google Yahoo Ask Jeeves About Overture Altavista Learn More

Web search results for "RSA "chinese remainder" public private" (1 - 20 of 29)

Refine Your Results

1. Cashing in on the Vulnerabilities of Cash Cards
... that they could unravel one form of a **public**-key digital signature scheme, an implementat **RSA** system based on the **Chinese remainder** theorem (CRT ...
http://www.siam.org/siamnews/general/cards.htm

2. **RSA Public**-Key Encryption
... Euler and Fermat, and upon the **Chinese Remainder** Theorem, which ... encrypted with a user's **public**-key procedure ... as the inverse of e. The **RSA** system works ...
http://www.ius.edu/ComputerScience/Projects/b438/Gary.htm

3. Class iaik.security.**rsa**.RSAPrivateKey
... byte[], encode() Returns this **RSA private** key as ... BigInteger, getCrtCoefficient() Return **Chinese Remainder** Theorem coefficient ... Returns the **public** exponent of ...
http://www.cs.utexas.edu/users/chris/cs378/f98/resources/iai...

4. Interface javax.crypto.interfaces.RSAPrivateKeyCrt
... **public** interface RSAPrivateKeyCrt extends RSAPrivateKey ... to be implemented for suppor **private** keys using the **Chinese Remainder** Theorem(CRT ...
http://www.cs.utexas.edu/users/chris/cs378/f98/resources/iai...

5. RFC 3447 - **Public**-Key Cryptography Standards (PKCS) #1: **RSA**
...observed the benefit of applying the **Chinese Remainder** Theorem to **RSA** operations. ... s process data with an **RSA public** or **private** key, and...
http://rfc.sunsite.dk/rfc/rfc3447.html

6. PKCS #1 v2.0 Amendment 1: Multi-Prime **RSA**
... and signature schemes and the **public**-key operations ... The benefit of multi-prime **RSA** is primitives, provided that the CRT (**Chinese Remainder** Theorem) is ...
http://mirror.switch.ch/ftp/doc/standard/pkcs/pkcs-1/pkcs-1v...

7. Copyright (C) 2000 **RSA** Security Inc. License to copy this document ...
... and signature schemes and the **public**-keyoperations and ... The benefit of multi-prime **RS** lower ... primitives, provided that the CRT (**Chinese Remainder** Theorem) is ...
http://mirror.switch.ch/ftp/doc/standard/pkcs/pkcs-1/pkcs-1v...

8. Twenty Years of Attacks on the **RSA** Cryptosystem
... N, e be an **RSA public** key. Given the. **private** key ... By the **Chinese Remainder** Theore four ...
http://www.ams.org/notices/199902/boneh.pdf

9. This file is THEORY from rpem.tar.Z Available from dcssparc.cl.msu ...
... root algorithm, coupled with the **Chinese Remainder** Theorem, is ... edu> Subject: Re: R **public** key algorithm ... probably equivalent to or better than **RSA**. ...
http://www.funet.fi/pub/crypt/cryptography/rpem/rpem/THEORY

10. PGP DH vs. **RSA** FAQ
...to speed up computation via the **Chinese remainder** theorem ... signature (irrespective of **public/private** key size). In contrast, **RSA** signature...
http://www.scramdisk.clara.net/pgpfaq.html

11. cs542 lecture 3-11-97
CS 542-002 (Cheng) Class Notes 3-11-97. The **RSA** Cryptographic System. In order for two u make encrypted communication on a **public** channel, they must share a secret key. ... m, put as its **RSA public** key and keep (d,n) as its **RSA private** key ... a special form of the **Chines remainder** theorem (100 AD). x=a ...
http://cheng.ececs.uc.edu/cs542/3-11.html

12. **rsa**.c - **RSA** function * Copyright (c) 1997,1998,1999 by Werner Koch ...

... if(g10m_cmp(test, out2)) g10_log_fatal("**RSA** operation: secret ... n, p, q); /* find a **pu** exponent */ e ... of p and q (used for **chinese remainder** theorem)*/ u ...
http://ftp.gnupg.zone-h.org/contrib/rsa.c

13. Java Cryptography Architecture
... KeyFactory supplies a DSA **private** or **public** key (from its encoding ... class) specifies an **I private** key, as defined in the PKCS#1 standard, using the **Chinese Remainder** Theorem (CI
http://www.warmi.net/docs/java/docs/guide/security/CryptoSpe...

14. Smart Cards and **Private** Currencies
...algorithms, allows for **RSA** key ... with its own **private** key (of a **private** key/**public** key ... through the use of the **Chinese Remainder**...
http://www.aci.net/kalliste/smartcards.htm

15. Twenty Years of Attacks on the **RSA** Cryptosystem
.. be an **RSA public** key. Given the **private** key ... By the **Chinese Remainder** Theorem, 1 square roots modulo ...
http://theory.stanford.edu/~dabo/papers/RSA-survey.pdf

16. RFC 2313 - PKCS #1: **RSA** Encryption Version 1.5. B. Kaliski.
...for **RSA public** and **private** ... q-1). o coefficient is the **Chinese Remainder** Theorem coef mod p. Notes. 1. An **RSA private** key logically...
http://sunsite.dk/RFC/rfc/rfc2313.html

17. RFC 2313 (rfc2313) - PKCS #1: **RSA** Encryption Version 1.5
...for **RSA public** and **private** ... q-1). o coefficient is the **Chinese Remainder** Theorem coef mod p. Notes. 1. An **RSA private** key logically...
http://www.faqs.org/rfcs/rfc2313.html

18. CS 6623, Data Security
... Kaufman, Perlman and Speciner, Network Security: **Private** Communication in a **Public** W(Prentice-Hall, 1995. ... Applications of number theory to **RSA**. **Chinese remainder** theorem .
http://www.csm.astate.edu/~rossa/cs6623.html

19. Name (Print) _____..
... n would be different for different people's **public** keys ... 2, since the **Chinese Remainder** could be used to find m ... some random bytes as part of **RSA** messages ...
http://users.ece.gatech.edu/~copeland/jac/6086/quiz-1_ans.pd...

20. CJ Request for the book Applied Cryptography
Fort Myer Drive Arlington, VA 22209-3113 Fax +1 703 875 5845 ATTN: 15 Day CJ Request Co National Security Agency P.O. ... **private** key, 35 hardware vs. software, 181, 83 introduction knapsack algorithm, 279 multiple, 165, 69 one-time pads, 13, 16 probabilistic, 406, 8 **public-RSA** ...
http://people.qualcomm.com/karn/export/book-cjr.html

Web search results for "RSA "chinese remainder" public private" (1 - 20 of 29)